(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 June 2004 (17.06.2004)

PCT

(10) International Publication Number
WO 2004/051482 A3

(51) International Patent Classification[7]: G06F 12/14, 1/00

(21) International Application Number:
PCT/IB2003/005271

(22) International Filing Date:
19 November 2003 (19.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
102 56 587.2 4 December 2002 (04.12.2002) DE

(71) Applicant *(for DE only)*: **PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(71) Applicant *(for all designated States except DE, US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FEUSER, Markus** [DE/DE]; c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE). **SOMMER, Sabine** [DE/DE]; c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

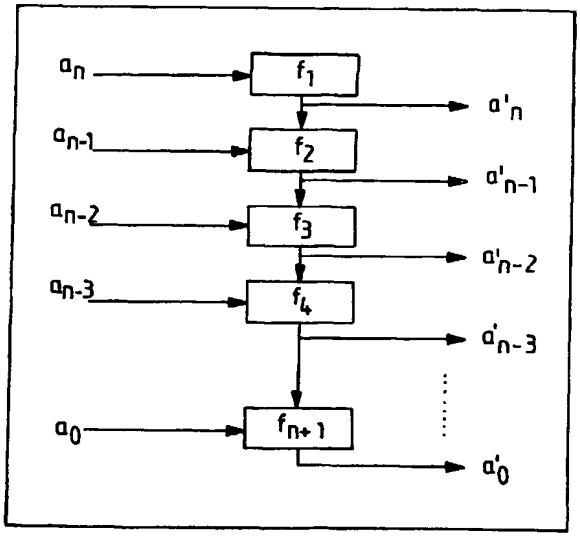
(74) Agent: **MEYER, Michael**; Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: ADDRESS ENCRYPTION METHOD FOR FLASH MEMORIES



(57) Abstract: In order to further develop a data processing device, in particular an electronic memory component, comprising a plurality of access-secured sub-areas, in particular a plurality of access-secured memory areas, each having at least one assigned parameter (a_n, a_{n-1},..., a_1, a_0), in particular address, and a method of encrypting at least one parameter (a_n, a_{n-1},..., a_1, a_0), in particular the address, of at least one access-secured sub-area, in particular at least one access-secured memory area, of at least one data processing device, in particular at least one electronic memory component, in such a way that on the one hand the security of such devices is increased considerably and on the other hand the associated expense and technical complexity are not too great, it is proposed that the parameter (a_n, a_{n-1},..., a_1, a_0) of at least one sub-area be capable of encryption only in certain areas, i.e. in dependence on least one further sub-area (a'_n, a'_{n-1},..., a'_1, a'_0).

WO 2004/051482 A3

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
25 November 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F12/14 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 908 810 A (GEN INSTRUMENT CORP) 14 April 1999 (1999-04-14) abstract; figures 1,2,6 paragraphs '0004!, '0009!, '0015!, '0027!, '0033!, '0035!, '0040!, '0050! - '0055!, '0057!, '0061!, '0103!, '0108! - '0115!, '0117!, '0122! paragraphs '0133! - '0135!, '0137! - '0140!, '0145!, '0164! - '0167!, '0169! - '0172!, '0177!, '0182! paragraphs '0190! - '0194!, '0199!, '0222!, '0229!	1-7,9,10

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 September 2004	28/09/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Breche, P

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 081 675 A (KITTIRUTSUNETORN KITTI) 14 January 1992 (1992-01-14) abstract; figures 2.a.1-8.2 column 1, lines 35-49 column 4, lines 22-36 column 5, lines 19-29,32-42,44-62 column 6, lines 7-39 column 6, line 64 - column 7, line 2 column 7, lines 15-40 column 9, lines 35-37 column 10, lines 11-13,59-64 column 11, line 54 - column 12, line 40 column 12, lines 46-68 column 13, lines 34-52,54-63 column 14, lines 44-66 column 15, line 56 - column 16, line 3 column 17, lines 55-58 column 17, line 63 - column 18, line 40 column 19, lines 1-29,50-61 column 20, lines 20-24,35-58	1-7,9,10
X	US 2001/037450 A1 (UTYANSKY DMITRY B ET AL) 1 November 2001 (2001-11-01) abstract; figures 4-6,9,12 paragraphs '0030!, '0041!, '0047!, '0056!, '0057!, '0108!, '0109!, '0113!, '0121! - '0123!, '0129!, '0154!, '0156!, '0159! paragraphs '0164! - '0166!, '0181!, '0204!; claim 9	1,3-6,9, 10
X	DAEMEN J ET AL: "On the design of high speed self-synchronizing stream ciphers" SINGAPORE ICCS/ISITA '92. 'COMMUNICATIONS ON THE MOVE' SINGAPORE 16-20 NOV. 1992, NEW YORK, NY, USA,IEEE, US, 16 November 1992 (1992-11-16), pages 279-283, XP010066981 ISBN: 0-7803-0803-4 abstract paragraphs '0001!, '0002!, '02.2!, '0004! - '0006!, '06.1!, '06.2!	1-7,9,10
A	EP 0 617 383 A (MOTOROLA INC) 28 September 1994 (1994-09-28) the whole document	1-7,9,10

INTERNATIONAL SEARCH REPORT

nternational application No.
PCT/IB 03/05271

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 8
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 8

The wording of claim 8 is not clear and is not understood in the light of the description (Article 6 PCT). Said claim has been therefore not searched.

The definitions of claims 1-7, 9-10 and their support in the description are so unclear that a partial search has been performed for the following reasons:
a) The many occurrences of the wording "in particular" in the claims, the wording "i.e in dependence on at least one further sub-area" in independent claims 1 and 6, the absence of formal definition of the encryption function in the claims and in the description (no mathematical formulae clearly specifies the encryption algorithm), ambiguities on the object to be encrypted (what is a secured sub-area with an assigned parameter: a memory location within a given memory or a memory among other memories? Is the address stored encrypted in a memory location or is the address scrambled when accessing a memory location? Is ai an address word of a data word stored in memory as suggested by page 5 or, the ith bit of an address word as suggested by page 1, lines 18-22), the absence of support in the description to clarify it unambiguously, the absolute non compliance to Article 5.1a)(I-v) (no clear background, no reference to attack or countermeasure, no reference cited in the domain, no attempt to put the encryption formulae into perspective with the numerous known algorithms and implementations, no clear problem defined, ambiguities of the "solution", no technical effect taught but scrambling of (an, ... , a0) - see in particular the logomachy on page 1, lines 9-page 2, lines 6) which might have helped to identify the kind of attack, countermeasure or encryption implementation, make it difficult, if not impossible, to determine the matter for which protection is sought - but encryption of some data following a generic algorithm - , and place an undue burden on others seeking to establish the extent of the protection and on searching prior art.
b) present claims 1, 2, 6 and 7 relate to method/apparatus defined (inter alia) by reference to an assigned parameter as claimed in claims 1 and 6 and to a formulae (not formally defined) as disclosed in claims 2 and 6. The use of a parameter and of a "pseudo" formula in the present context is considered to lead to a lack of clarity within the meaning of Article 6 PCT. It is impossible to compare said parameter and "pseudo" formulae the applicant has chosen to employ with what is set out in the prior art. The lack of clarity is such as to render a meaningful complete search impossible (see PCT Guidelines C.III.9.01, 9.19, 9.22, 9.24 C.IV, 15.18, 15.22, 15.29). Consequently, the search has been restricted to the domain of secure IC and smart cards using encryption/scrambling as follows:
. attack: SPA and DPA analysis,
. countermeasure: address protection for non volatile memory based on address scrambling only (page 2, lines 16-27, page 5 is interprated as scrambling n+1 bits representing the address word of a data word stored at a memory location in a non volatile memory),

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

. stream cypher based algorithms (see on page 2, lines 24-26, page 5, and figure 1) and, as far as possible, functions expressed recursively with cascading functions.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.5), should the problems which led to the Article 17(2) declaration be overcome.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0908810 A	14-04-1999	US 6061449 A	09-05-2000
		CA 2249554 A1	10-04-1999
		CN 1236132 A	24-11-1999
		EP 0908810 A2	14-04-1999
		IL 126448 A	14-08-2002
		TW 445402 B	11-07-2001
US 5081675 A	14-01-1992	NONE	
US 2001037450 A1	01-11-2001	AU 4336501 A	12-09-2001
		WO 0165366 A1	07-09-2001
EP 0617383 A	28-09-1994	GB 2276254 A	21-09-1994
		CN 1102265 A ,B	03-05-1995
		EP 0617383 A2	28-09-1994
		HK 1003850 A1	06-11-1998
		JP 7006096 A	10-01-1995
		SG 52302 A1	28-09-1998
		US 5563945 A	08-10-1996